



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/826,320	04/03/2001	Gary Liu	10664-147001	4156
26181	7590	11/05/2004	EXAMINER	
FISH & RICHARDSON P.C. 3300 DAIN RAUSCHER PLAZA MINNEAPOLIS, MN 55402			ELISCA, PIERRE E	
		ART UNIT		PAPER NUMBER
		3621		

DATE MAILED: 11/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	09/826,320	LIU, GARY
	Examiner	Art Unit
	Pierre E. Elisca	3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 29 September 2004.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-51 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) 22 and 23 is/are allowed.
- 6) Claim(s) 1-21 and 24-51 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) All    b) Some \* c) None of:
    1. Certified copies of the priority documents have been received.
    2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |                                                                                                                        |                                                                             |
|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                                                       | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | Paper No(s)/Mail Date. _____                                                |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
|                                                                                                                        | 6) <input type="checkbox"/> Other: _____                                    |

## DETAILED ACTION

1. This Office action is in response to Applicant's RCE, filed on 9/29/2004.
2. Claims 1-51 are pending.

### ***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371<sup>©</sup> of this title before the invention thereof by the applicant for patent.

4. Claims 1-21 and 24-51 are rejected under 35 U.S.C. 102(2) as being anticipated by Al-Salqan (U.S. Pat. No. 6,549,626).

As per claims 1, 4-9, 10-21 and 24-51 Al-Salqan discloses a key such as a private key or key password of a private key is encrypted for storage, and may be decrypted if the private key becomes lost or unavailable. The key is encrypted by encoding, for example, by using hashing, private information, and the result is used as a key to encrypted the private key DES, comprising:

encrypted a message using a symmetric key to generate an encrypted message (see., abstract, col 2, lines 49-64, col 1, lines 29-38, specifically wherein it is stated that a message transmitted from sender to recipient may be symmetrically encrypted); sending the encrypted message to an intended recipient without making the symmetric

key immediately accessible to the intended recipient (see., abstract, col 2, lines 49-64, col 1, lines 29-38, specifically asymmetric encryption or private/public keys); providing the symmetric key to a third party (see., col 1, lines 51-67, specifically wherein said a trusted party known as a certificate authority issues a certificate which allows third parties to verify the identity of the principal, please note that principal or private/public keys or symmetric key or DES); and if the intended recipient signs and returns to the third party a receipt (or certificate) including a representation of the encrypted message, transferring by the third party, the receipt to a sender and providing the symmetric key to the intended recipient (see., abstract, col 1, lines 29-38, and lines 51-67, specifically wherein it is stated that a trusted party known as a certificate authority issues a certificate which allows third parties to verify the identity of the principal, please note that principal or private/public keys or symmetric key or DES, and abstract, specifically wherein said to decrypt the key recovery file, the private key corresponding to the public key used to encrypt the key recovery filed is used to decrypt the key recovery file. The result is symmetrically decrypted using a key obtained by encoding).

As per claim 2, Al-Salqan discloses the claimed method wherein the receipt signed by the recipient contains an identifier computed from the message and the symmetric key using cryptographically secure hash functions (see., col 1, lines 50-67, col 4, lines 47-67).

As per claim 3, Al-Salqan discloses a key such as a private key or key password of a

private key is encrypted for storage, and may be decrypted if the private key becomes lost or unavailable. The key is encrypted by encoding, for example, by using hashing, private information, and the result is used as a key to encrypted the private key DES, comprising:

at the sender, encrypted a message using a symmetric key, encrypting the symmetric key to make the symmetric key accessible to a third party but not immediately accessible to an intended recipient and sending the encrypted message and the encrypted symmetric key to the intended recipient (see., abstract, col 2, lines 49-64, col 1, lines 29-38, specifically wherein it is stated that a message transmitted from sender to recipient may be symmetrically encrypted);

at the recipient, signing a receipt including a representation of the encrypted message and sending the receipt and the encrypted symmetric key to the third party (see., abstract, col 2, lines 49-64, col 1, lines 29-38, specifically asymmetric encryption or private/public keys);

at the third party, transferring the receipt to the sender and providing the symmetric key to the intended recipient if the receipt (or certificate) is properly signed (see., col 1, lines 51-67, specifically wherein said a trusted party known as a certificate authority issues a certificate which allows third parties to verify the identity of the principal, please note that principal or private/public keys or symmetric key or DES, see., abstract, col 1, lines 29-38, and lines 51-67, specifically wherein it is stated that a trusted party known as a certificate authority issues a certificate which allows third parties to verify the identity of the principal, please note that principal or private/public keys or symmetric key or DES,

and abstract, specifically wherein said to decrypt the key recovery file, the private key corresponding to the public key used to encrypt the key recovery file is used to decrypt the key recovery file. The result is symmetrically decrypted using a key obtained by encoding).

***Allowable Subject Matter***

5. Claims 22 and 23 are allowed over the prior art of record.

***Conclusion***

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pierre E. Elisca whose telephone number is 703 305-3987. The examiner can normally be reached on 6:30 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 703 305-9769. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Pierre Eddy Eliscsa

**Primary Patent Examiner**

**November 03, 2004**